U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: Guidance Material for 14 CFR § 35.23, Propeller Control System	**Date:** DRAFT **Initiated by:** ANE-110	**AC No:** DRAFT AC 35.23 **Change:**

1. Purpose. This advisory circular (AC) provides definitions and guidance for demonstrating compliance with the propeller control system requirements of Title 14 of the Code of Federal Regulations (14 CFR 35.23).

2. Applicability.

a. The guidance provided in this document is directed to propeller manufacturers, modifiers, and foreign regulatory authorities.

b. This material is neither mandatory nor regulatory in nature and does not constitute a regulation. It describes acceptable means, but not the only means, for demonstrating compliance with the applicable regulations. The FAA will consider other methods of demonstrating compliance that an applicant may elect to present. Terms such as "should," "shall," "may," and "must" are used only in the sense of ensuring applicability of this particular method of compliance when the acceptable method of compliance in this document is used. While these guidelines are not mandatory, they are derived from extensive FAA and industry experience in determining compliance with the relevant regulations. On the other hand, if the FAA becomes aware of circumstances that convince us that following this AC would not result in compliance with the applicable regulations, we will not be bound by the terms of this AC, and we may require additional substantiation as the basis for finding compliance.

c. This material does not change, create any additional, authorize changes in, or permit deviations from existing regulatory requirements.

3. Related Reference Material.

a. Relevant Regulations. 14 CFR §§ 23.901, 23.905, 23.1309, 25.901, 25.905, 25.1309, 33.19, 35.3, 35.4, 35.15, 35.21, 35.23, 35.42, 35.43, and Appendix A of part 35.

b. FAA Documents.

(1) AC 20-115B, RTCA Inc., Document RTCA/DO-178B; January 11, 1993.

(2) AC 20-136A, Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning; December 21, 2006.

(3) AC 20-152, RTCA Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware; June 30, 2005.

(4) AC 20-158, The Certification of Aircraft Electrical and Electronic Systems for Operation in the High-Intensity Radiated Fields (HIRF) Environment; July 30, 2007.

(5) AC 21-16E, RTCA, Inc. Document RTCA/DO-160E, Environmental Conditions and Test Procedures for Airborne Equipment; December 20, 2005.

(6) AC 23.1309-1C, Equipment, Systems, and Installations in Part 23 Airplanes; March 12, 1999.

(7) AC 25.1309-1A, System Design and Analysis; June 6, 1988.

(8) AC 35-1, Certification of Propellers; December 29, 2008.

(9) FAA Order 8110.49, Software Approval Guidelines; June 2, 2003.

(10) FAA Order 8110.105, Simple and Complex Electronic Hardware Approval Guidance; September 23, 2008.

c. European Aviation Safety Agency (EASA) Advisory.

(1) AMC 20-115B, General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances, Recognition of EUROCAE ED-12B/RTCA DO-178B, November 5, 2003.

(2) EASA Certification Specifications for Propellers (CS-P) Amendment 1; November 16, 2006.

d. Industry Documents.

(1) International Electrotechnical Commission (IEC).

(a) IEC/TS 62239, Process Management for Avionics – Preparation of an Electronic Components Management Plan, First edition 2003-05.

(b) IEC/TR 62240, Process Management for Avionics - Use of Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges, First edition 2005-06.

(2) RTCA Documents.

(a) RTCA DO-178B/EUROCAE ED-12B, Software Considerations in Airborne Systems and Equipment Certification; December 1992.

(b) RTCA DO-254/EUROCAE ED-80, Design Assurance Guidance for Airborne Electronic Hardware; April 19, 2000/April 2000.

(c) RTCA/DO-160F/EUROCAE ED-14F, Environmental Conditions and Test Procedures for Airborne Equipment; December 6, 2007/March 2008.

(3) SAE International.

(a) SAE ARP5107A, Guidelines for Time Limited Dispatch (TLD) Analysis for Electronic Engine Control Systems; January 2005.

(b) SAE ARP5415A/EUROCAE ED-91, Users Manual for Certification of Aircraft Electrical/Electronic Systems for the Indirect Effects of Lightning; May 2002.

(c) SAE ARP5416/EUROCAE ED-105, Aircraft Lightning Test Methods; March 2005/April 2005.

(d) SAE ARP5583, Guide to Certification of Aircraft in a High Intensity Radiated Field (HIRF) Environment; January 2003.

(e) SAE ARP5757, Guidelines for Engine Component Tests; March 2008.

(f) SAE ARP5890, Guidelines for Preparing Reliability Assessment Plans for Electronic Engine Controls; November 2002.

e. Military Specifications.

(1) MIL-STD-461E, Requirements for the Control of Electromagnetic Interference Characteristics; August 20, 1999.

(2) MIL-STD-810E or F, Test Method Standard for Environmental Engineering; July 14, 1989.

(3) MIL-STD-810F, Test Method Standard for Environmental Engineering; January 1, 2000.

(4) MIL-E-5007E, Engines, Aircraft, Turbojet and Turbofan, General Specification For; September 1, 1983.

f. Reference Addresses. The following addresses are provided to aid in accessing some of the reference documents. The addresses are subject to change.

(1) EASA documents are available online at: http://www.easa.eu.int.

(2) FAA documents are available online at: http://www.faa.gov.

(3) IEC documents are available at: IEC, Central Office, 3, rue de Varembé, P.O. Box 131, CH - 1211 GENEVA 20, Switzerland. They are also available online at: http://www.iec.org.

(4) MIL STD documents may be available online at: http://www.dtc.army.mil.

(5) RTCA documents are available at: RTCA, Inc. 1828 L Street, NW, Suite 805, Washington, DC 20036 or EUROCAE, 17, rue Hamelin, 75116, Paris, France. Also available online at: http://www.rtca.org or http://www.eurocae.org.

(6) SAE documents are available at: SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001 USA or EUROCAE, 102, rue Etienne Dolet, 92240, Malakoff, France. Also available online at: http://www.sae.org.

4. Definitions. For the purposes of this AC, the following definitions apply:

a. Airplane-supplied data. Data supplied by or via airplane systems.

b. Airplane-supplied electrical power. Any electrical power supplied by or via airplane systems and used by the engine or propeller control system. Engine supplied power is a subset of airplane-supplied power.

c. Airborne Electronic Hardware (AEH). (As defined in RTCA DO-254) includes line replaceable units, circuit board assemblies, application specific integrated circuits, programmable logic devices, etc.

d. Alternate mode. Any control mode that is not the primary mode.

e. Analysis and assessment. The two terms are, to some extent, are interchangeable. However, "analysis" generally implies a specific and detailed evaluation, while "assessment" implies a general or broader evaluation that may include one or more types of analysis. In practice, the distinction comes from the specific application (for example, Functional Hazard Analysis (FHA), Fault Tree Analysis (FTA), Markov Analysis, or Preliminary System Safety Assessment (PSSA)).

f. Back-up mode. The back-up system control mode. The alternate channel in a dual channel system with identical channels is not a back-up mode. Any additional back-up means provided differing from the two channels are back-up modes under the definition.

g. Back-up system. A part of the engine or propeller control system where the operating characteristics or capabilities of the propeller control are sufficiently different from the primary system that the operating characteristics or capabilities of the airplane, crew workload, or what constitutes appropriate crew procedures may be significantly impacted or changed.

h. Control mode. Each defined operational state of the propeller control system in which the crew can exercise satisfactory propeller control, which may involve evaluation in the airplane.

i. Covered fault. A fault that is detected or accommodated.

j. Dedicated power source. A dedicated power source is defined as an electric power source that provides electrical power generated and supplied solely for use by a single propeller control system.

k. Dispatchable Configuration. All control system configurations approved for dispatch.

l. Electronic propeller control system (EPCS). A propeller control system in which the primary functions are provided using electronics. It includes all the components (for example, electrical, electronic, hydro-mechanical and pneumatic) necessary for the control of the propeller and may incorporate other control functions where desired. Components of the system provided by the installer may be considered part of the system.

m. Engine control system (ECS). Any system or device that controls, limits, or monitors engine operation.

n. Engine-supplied data. All data supplied by or via engine systems and used by the EPCS. Engine-supplied data is a subset of airplane-supplied data.

o. Error. An omission or incorrect action by a person, a mistake in requirements, design or implementation. An error may result in a failure, but an error is not a failure in and of itself.

p. Failure condition. A condition with direct, consequential propeller-level effects caused or contributed to by one or more failures.

q. Failure mode. The cause of the failure or the manner in which an item or function can fail. Examples include failures due to corrosion or fatigue, opens and shorts in circuits, and malfunctions of electronic components.

r. Fault (or) failure. A condition where the operation of a component, part, or element can no longer function as intended, including loss of function.

s. Fault (or) failure accommodation. The capability to mitigate, in either full or in part, the effects of a fault or failure.

t. Full authority digital engine control (FADEC). An engine control system in which the primary functions use digital electronics and the electronic engine control (EEC) unit has full-range authority over the engine power or thrust. A FADEC may incorporate the propeller control functions.

u. Full-up configuration. An EPCS that has no known faults or failures present.

v. Local events. These are failures of airplane systems and components, other than the EPCS, that may affect the installed environment of the EPCS.

w. Primary mode. The mode for controlling the propeller under normal operation; often referred to as the 'normal mode.'

x. Primary system. The part of the engine or propeller control system normally used for controlling the engine or propeller operation.

y. Programmable logic device (PLD). An electronic component that is altered to perform an installation specific function. PLDs include, but are not limited to, programmable array logic (PAL) components, general array logic (GAL) components, field programmable gate array (FPGA) components, and erasable programmable logic devices (EPLDs). These devices are a subset of AEH.

z. Propeller control system. Any system or device within the propeller system that controls, limits, or monitors propeller operation and is necessary for the continued airworthiness of the propeller.

aa. Redundancy. Multiple independent methods incorporated within a system to accomplish a given function.

bb. Uncovered fault. A fault or failure for which either no detection mechanism exists or, if detected, no accommodation exists.

5. Background.

a. The purpose of § 35.23 is to set objectives for the general design and functioning of the propeller control system. These requirements do not replace or supersede other requirements. Therefore, individual components of the control system, such as pumps, sensors, and actuators, should also be addressed in other paragraphs of part 35, such as § 35.42 Components of the propeller control system and § 35.43 Propeller hydraulic components, as appropriate. Also, § 35.21 Variable and reversible pitch propellers and § 35.22 Feathering propellers provide specific requirements for propellers that provide these features.

b. When part 35 was updated to amendment 8, changes were also made to parts 23, 25 and 33. Sections 23.905(d), 25.905(c), and 33.19(d) were modified to assure that propeller control systems included in the airplane or engine type design are subjected to equivalent requirements. The specific part 35 requirements are §§ 35.21, 35.23, 35.42 and 35.43. These requirements are applicable to an airplane or engine as follows:

(1) The propeller control system requirements are applicable when new propeller controls are included in an airplane or engine type certificate (TC), amended TC or supplemental type certificate (STC).

(2) The propeller control system requirements are not applicable when a certified propeller is installed on a new or amended airplane TC or an STC and propeller control system has not changed.

6. Section 35.23 - General.

a. One of the objectives for the propeller manufacturer in a propeller certification program is to show that the certificated propeller is "installable" in a particular airplane or airplane type. Parts 23 and 25 provide regulations for the installation of a certificated propeller into an airplane. The installed propeller becomes a part of the powerplant system. These regulations require the powerplant system design meet all the requirements, procedures, limitations, and assumptions specified in the propeller installation or operating instructions and the propeller type certificate data sheet (TCDS) or STC. We recognize that the determination of compliance of the propeller control system with applicable airplane certification regulations will only be made during airplane certification. As part of the airplane certification program, the FAA may require flight-testing to fully evaluate the propeller performance and operability characteristics for all operating modes relating to the applicable airplane certification regulations. When the airplane application is unknown at the time of propeller certification, the propeller manufacturer should make a reasonable installation and operational assumptions for the target application. Any installation limitations or operational issues must be noted in the propeller installation or operating instructions and/or the TCDS.

b. Propeller and airplane manufacturers should coordinate with the relevant authorities.

c. Where it is known or expected that airplane components, which are not part of the propeller type design, will contribute to or cause the failure conditions being evaluated in a part 35 safety analysis, the maximum allowable contribution from those additional airframe/engine components should be accounted for, both within the part 35 safety analysis and the installation limitations and instructions to assure the propeller will be installable. Where the installation is known, an agreement should be reached on the acceptance threshold for propeller control system failure rates.

d. The severity of propeller control system malfunctions increases with the complexity of the control and the range of pitch change permitted by the propeller control system. Most single engine general aviation airplanes use a control system with mechanical high and low pitch stops

that limit pitch control failures to these mechanical stops. These stops are typically set to a fail-safe pitch. However, these control systems do not permit reverse thrust or feathering. When the control system introduces reverse thrust and feathering, the range of permissible pitch increases from about 10 to 40 degree limits to about -15 to 90 degree limits with an in-flight low pitch stop of about 10 degrees. For all propellers flight operation below the in-flight low pitch stop is hazardous. §35.21 Variable and reversible pitch propellers provides additional requirements to prevent operation below the in-flight pitch position. With mechanical stops, some of the failures considered are the structural failure of the stop, miss-assembly of the stop, or improper setting of the stop. With reversing and feathering systems the control system typically involves a control mode transition from flight forward thrust operation to ground taxi and reverse thrust operation. In addition, the control must be designed to prevent hazardous unintended travel below the in-flight low pitch stop.

7. Section 35.23 - Applicability.

a. The regulation applies to all types of propeller control systems. These might be mechanical, hydro-mechanical, hydro-mechanical with a limited authority electronic supervisor, single channel full authority propeller control with hydro-mechanical back-up, or dual channel full authority electronic propeller control or any other combination. The electronic technology can be analog or digital.

b. This guidance applies to propeller certification for designs ranging from applications used on single reciprocating engine airplanes certified under part 23 to those used on multi-engine transport airplanes certified under part 25.

c. This guidance applies to primary propeller control of pitch and rotational speed as well as other functions, such as syncrophasing control, which may be integrated into the system for noise abatement, vibration abatement, or both.

d. Although this AC is applicable to all propeller control systems, the majority of the guidance provided in this AC is associated with electronic propeller control systems since they are much more susceptible to environmental effects, rely on airplane supplied power and data, and require software or airborne electronic hardware.

8. Section 35.23(a)(1) – Control Modes and Transitions.

a. <u>General</u>.

(1) The applicant should perform all necessary testing and analysis to ensure that all control modes function as intended. All declared dispatchable control modes should perform their intended functions in the environmental conditions, including but not limited to, high intensity radiated fields (HIRF) and lightning, declared in the propeller instructions for installation.

(2) The primary or normal mode includes all control functions designed for the intended control of the propeller. These control functions may include governing, beta control, feathering,

and the transitions between the various primary mode control functions. Operation in an alternate mode occurs for fault accommodation when propeller control moves from the primary mode to an alternate or back-up mode.

(3) The applicant should describe the functioning of the propeller control system in its primary and any alternate modes in the propeller instructions for installation and operation. The applicant should also clearly state any limitations on operations in alternate modes in this manual.

(4) Analyses, testing, or both are necessary to substantiate that transferring operation to alternate modes has no unacceptable effect on propeller durability or endurance. The applicant may demonstrate the durability and reliability of the control system in all modes by component testing. Performing some portion of the propeller testing in the alternate mode(s) and during transition between modes can be used as part of the system validation.

(5) All dispatchable control modes should be declared. If the applicant wants to dispatch with the propeller in an alternate mode, all relevant subsequent single failures must be considered and demonstrate no threat to continued safe flight and landing.

b. Propeller Test Considerations.

(1) The applicant may use the propeller endurance test and functional tests defined in §§ 35.39 and 35.41 using the primary full-up control system. The applicant, however, should demonstrate by test and/or analysis based on test, that the propeller can meet the defined criteria when operating in any alternative or back-up control mode. Adding some portion to the propeller endurance test and functional test in the alternate or back-up mode(s), including transition between modes, can be used as part of system validation, if desired. The component testing of § 35.42 addresses the durability of the control system.

(2) If the applicant performs propeller certification tests using only the propeller control system's primary mode in the full-up configuration, and is requesting approval for dispatch in the alternate mode, then the applicant should demonstrate by analysis, test, or both, the propeller can meet the defined test success criteria when operating in any alternate mode that is proposed as a dispatchable configuration.

(3) The capabilities in paragraph 8.b.(2) above may be lost in some control modes that are not dispatchable. These modes do not require propeller test demonstration under the adverse conditions for which they have lost capabilities as long as the installation instructions reflect this loss of capability.

c. Back-up Mode Availability. If the applicant claims there is no control degradation for a back-up mode which is not normally exercised, then the availability of such a back-up mode must be established by routine testing or monitoring to ensure it will be available when needed. The applicant should document the minimum frequency of inspection of testing needed to ensure the availability of the back-up mode in the instructions for continued airworthiness (ICA).

d. Control Transitions.

(1) In general, the propeller control system should transition to alternate modes automatically. However, systems in which pilot action is required to engage the back-up mode may also be acceptable. When pilot action is required, applicants must ensure that any reliance on manual transition does not pose an unacceptable operating characteristic, unacceptable crew workload, or require exceptional skill.

(2) The applicant should evaluate the transient change in speed or torque associated with transfer to alternate modes for acceptability. If available, input from the installer should be considered. Although not a complete list, some of the items that the applicant should consider when reviewing the acceptability of control mode transitions are:

(a) Establishment of the frequency of occurrence of transfers to any alternate mode and of the capability of the alternate mode.

(b) Computed frequency of transfer rates should be supported with data from endurance or reliability testing, in service experience on similar propeller control system, or other appropriate data.

(3) The applicant should evaluate the magnitude of the speed and torque transients and should also declare the speed or torque change associated with the transition in the instructions for installing the propeller.

(4) The applicant should demonstrate, by simulation or other means, the ability of the propeller control system to control the propeller safely during the transition.

(5) The applicant should provide an analysis to identify those faults that cause control mode transitions either automatically or through pilot action.

(6) Control transitions that are the result of fault accommodation should occur in an acceptable manner.

e. Time Delays. The applicant should identify any observable time delays associated with control mode, channel or system transitions, or in re-establishing the pilot's ability to modulate propeller speed or torque, in the propeller instructions for installation and operation.

9. Section 35.23(a)(2) – Environmental Considerations.

a. The objective of this requirement is to demonstrate the control system can function in its installed environment and to declare those environmental limitations as part of the type design characteristics in the instructions for propeller installation and operation. The declared environmental conditions, including but not limited to, temperature, electromagnetic interference (EMI), HIRF, and lightning.

(1) When the installer specifies the environmental conditions of the installation, compliance with this requirement can be demonstrated by environmental testing meeting the specified installation requirements.

(2) When the installation requirements are not specified, the applicant should conduct environmental testing to demonstrate that the control system can be installed in a typical installation for which the control system is designed.

(3) Electronics may be sensitive to lightning and other EMI. Therefore, electronic controls are designed with protections to compensate for this sensitivity. For compliance, the system design should demonstrate the functional integrity of the control system when subjected to designated levels of electromagnetic disturbances.

(4) Hydro-mechanical and mechanical control systems have not been sensitive to lightning and other EMI. Compliance may be shown by similarity to existing designs with service experience.

b. Environmental Considerations.

(1) The use of general conditions, such as those of RTCA/DO-160F (see paragraph 3. d(2)(c) of this AC), allows certification of the EPCS in a consistent manner. For the purpose of this AC, RTCA/DO-160F will be referred to as DO-160F. However, installation on some airplanes may require additional considerations. Therefore, the applicant and airplane manufacturer should coordinate with each other, as well as with the appropriate FAA certification offices, to ensure the propeller installation is acceptable. Additional guidance is found in AC 20-136A and SAE ARP5757, which is more specific to engine components. It should be noted that MIL-STD-810 may be used when the tests are equal to or more rigorous than those defined in DO-160F. In addition, DO-160F falls a bit short in one area, temperature variation. A minimum of 10 temperature cycles should be performed for temperature variation tests.

(2) Radio Frequency (RF) Emission Test Procedures and Test Limits. The procedures and limits in MIL-STD-461 or DO-160F section 21 are acceptable.

(3) HIRF and Lightning Tests.

(a) Test Levels. The propeller control system should be tested with HIRF and lightning test levels determined and agreed upon by the propeller applicant and airplane manufacturer or modifier. The applicant should select these HIRF and lightning test levels so the installation meets the airplane certification regulations. The HIRF compliance regulations are in §§ 23.1308, and 25.1317, HIRF protection. FAA guidance on HIRF compliance is found in AC 20-158. The lightning compliance regulations are in §§ 23.1309(e) and 25.1316. FAA guidance on system lightning compliance is found in AC 20-136A. Successful completion of the propeller control system HIRF and lightning tests at these levels should be declared for propeller type certification and documented in the propeller installation instructions. The DO-160F section 20 and 22 categories and waveform sets defined in paragraph 9.b.(3)(a)*1* below should be used by the

propeller applicant if HIRF and lightning test levels have not been determined for a specific airplane and propeller installation.

1. Airplane Installation Relevance. The HIRF and lightning test levels are typically determined through lightning transient and HIRF attenuation characterization tests on the airplane with the propeller installed. If the HIRF and lightning test levels for the propeller installation on a particular airplane are not known at the time of the propeller certification, the propeller applicant may choose to use the HIRF and lightning test levels in paragraphs 9.b.(3)(a)2, 3, 4, and 5, below. However, these test levels should be confirmed by lightning transient characterization and HIRF attenuation tests on the airplane with the propellers installed before airplane certification. Additional propeller control system HIRF and lightning tests or analysis may be required if the airplane characterization shows that these test levels and waveform sets do not adequately represent the lightning transient and HIRF attenuation characteristics for the airplane and propeller installation. The propeller installation instructions should specify any wire shields, connectors, shield terminations, and electrical bonding that are required for HIRF and lightning protection when the propeller is installed on the airplane. The propeller control system HIRF and lightning tests should be performed with the same shielding and electrical bonding configuration.

2. HIRF Levels. The minimum levels for system laboratory HIRF conducted RF susceptibility tests should be DO-160F Category W (150 mA). The minimum levels for system laboratory HIRF radiated RF susceptibility continuous wave (CW) and square wave (SW) modulation tests should be DO-160F Category W (100 v/m). The minimum levels for system laboratory HIRF radiated RF susceptibility pulse modulation tests should be DO-160F Category D (up to 750 v/m).

3. Alternate HIRF Levels for propellers on airplanes with reciprocating engines. Using the HIRF test levels in paragraph 9.b.(3)(a)2 above combined with design requirements in paragraphs 9.b.(3)(a)3(aa), (bb), and (cc) below should be acceptable for airplane installation without further airplane HIRF tests. The propeller control system design and the instructions for installation should specify the following lightning protection features:

(aa) The propeller electronic control system should be installed in an airplane with engine cowls and a firewall that incorporate electrically conducting materials. The conducting materials may be aluminum, copper, steel or carbon fiber composites, and may include thin metal foil or mesh incorporated into non-conducting composites. The propeller electronic control system should be installed either under the conducting cowl or in the airframe that uses structure with similar conducting materials.

(bb) Required wire shielding and connectors for wire bundles that connect the propeller electronic control system to airplane systems should be specified. The required wire shielding and connectors should be used during the HIRF tests.

(cc) Electrical bonding requirements for the propeller electronic control system should be specified.

4. Lightning Levels. The minimum levels for system laboratory lightning tests should be DO-160F section 22 Level 3 for cable bundle injection tests and pin injection tests. The waveform set that includes single stroke, multiple stroke, and multiple burst waveforms for shielded wire bundles should be Category A3J33 in DO-160F section 22. Series impedance should not be used during the pin injection tests (DO-160F section 22.5.1.h) unless the remote load impedance is in a component included as part of the certified propeller. Electronic propeller control systems are subject to very high lightning transients when lightning attaches to the propeller, so higher lightning transient test levels may be required.

5. Alternate Lightning Levels for propellers on airplanes with reciprocating engines. Propeller electronic control systems for these types of airplane installations are normally subject to very high lightning transients when lightning attaches to the propeller. Using the lightning design and test requirements paragraphs 9.b.(3)(a)*5*(aa), and (bb), below, propeller electronic control systems should be acceptable for airplane installation without further airplane lightning tests. The minimum levels for system laboratory lightning tests should be DO-160F section 22 and should be Category A3G33 for unshielded wire bundles. The waveform set for these tests that includes single stroke, multiple stroke, and multiple burst waveforms is in DO-160F section 22. The propeller control system tests, design, and the instructions for installation should meet the following requirements:

(aa) Test setup. The test setup guidance in DO-160F section 22.3 should be used. The cable bundle injection tests should be performed with the propeller electronic control system wire bundle shields disconnected so the transients are injected directly onto the wires. Series impedance should not be used during the pin injection tests (DO-160F section 22.5.1.h) unless the remote load impedance is in a component included as part of the certified propeller.

(bb) Wire bundle shields. All wire bundles between propeller electronic control systems components, and from propeller electronic control systems components to the airplane should specify the use of overbraid shields. The shields should cover power and signal wires and their returns. The shield should have low resistance and high optical coverage. An overbraid shield may enclose an entire wire bundle, or multiple overbraid shields may be used over groups of wires within a bundle. The shields should be terminated to each connector. The shield terminations should be very short, preferably using backshells with zero length shield terminations. The connector shells and backshells should provide a very low resistance to the propeller components, FADEC, and airplane firewall or structure. Features required for electrically bonding the connectors to the airplane firewall or structure, such as surface preparation, should be specified in the instructions for propeller installation and operation.

(b) Test Procedures. The propeller control system used for the lightning and HIRF tests should include sensors, actuators, and propeller and propeller-airplane interface wire bundles. The applicant should use the HIRF and lightning test procedures provided in DO-160F sections 20 and 22. However, the test procedures defined in DO-160F, sections 20 and 22, are oriented to equipment tests. Further guidance on system level HIRF tests is available in SAE ARP5583. SAE ARP5415 and ARP5416 provide guidance on system level lightning tests.

(c) Open Loop and Closed Loop Testing. The applicant should conduct HIRF and lightning tests on the propeller control system operating in closed loop or open loop control. The closed loop set-up is usually provided with power to move actuators to close the inner actuating loops. A simplified propeller simulation may be used to close the outer propeller loop. HIRF and lightning tests should be conducted with the propeller control system controlling at the most sensitive operating point, as selected and detailed in the test plans by the applicant. The system should be exposed to the HIRF and lightning environments while operating at the selected condition. HIRF and lightning environments may have different sensitive operating points.

(d) Test Considerations. The following factors should also be considered:

1. If special propeller control system test software is used, that software should be developed and implemented by guidelines defined for software levels of at least Level C in DO-178B, or equivalent. In some cases, the application code is modified to include the required test code features;

2. The system test set-up should be capable of monitoring both the output drive signals and the input signals; and

3. Anomalies observed during open loop testing on inputs or outputs should be duplicated on the propeller simulation to determine whether the resulting power or thrust perturbations comply with the pass/fail criteria.

c. Pass/Fail Criteria. The environmental tests, EMI, HIRF and lightning, should cause no adverse effects on the functionality of the propeller control system. The following are considered adverse effects:

(1) A greater than +/- 3% change of rated speed from the normal control governing capability for a period of more than one second.

(2) Transfers to alternate channels, back-up systems, or alternate modes.

(3) Component damage.

(4) Significant fault codes recorded in the fault memory.

(5) False annunciation to the crew that could cause unnecessary or inappropriate crew action.

(6) Erroneous operation of protection systems, such as overspeed protection circuits.

d. Maintenance Actions.

(1) Section 35.4 requires the applicant to prepare ICA. Therefore, for any dedicated or inherent protection features that are part of the type design of the propeller control system and are

required to meet the qualified levels of EMI, HIRF and lightning, the applicant should provide a maintenance plan to ensure the continued airworthiness for the parts of the installed system supplied by the propeller TC holder.

(2) The maintenance actions considered include periodic inspections or tests for required structural shielding, wire shields, connectors, and EPCS protection components. The applicant should provide the engineering validation and substantiation of these maintenance actions.

10. Section 35.23(a)(3) – Flight Crew Action. In general, the propeller control system should transition to alternate modes automatically. However, systems in which pilot action is required to engage the back-up mode may also be acceptable. When pilot action is required, applicants must make certain that care is taken to ensure that any reliance on a pilot executing a manual transition does not pose an unacceptable operating characteristic, unacceptable crew workload, or require exceptional skill. If annunciation to the pilot is necessary, the type of annunciation should be appropriate with the nature of the transition. For example, when transition to an alternate mode of control is automatic and the only observable changes in operation of the propeller are different rotational speed settings, the annunciation is very different from when the pilot is required to take timely action to maintain control of the airplane. The instructions for propeller installation and operation should clearly state that assumed crew action and the acceptability of those crew actions should be evaluated during airplane certification.

11. Section 35.23(b) – Safety Assessment.

a. Airplane-Level Failure Classifications. Airplane-level failure classifications do not directly apply to propeller safety assessments because the airplane may have features that could decrease or increase the consequences of a propeller failure effect. Additionally, the same type-certificated propeller may be used in a variety of installations, each with different airplane-level failure classifications. The applicant should declare the type of airplane, such as a part 25 airplane or a part 23 single reciprocating engine airplane, on which the propeller control system will be installed. The applicant should also establish that the propeller failure modes and rates for certification and testing are at or above the airplane-level failure classifications. Otherwise, the propeller control system may not be of sufficient integrity for installation on the intended airplane. AC 23.1309 provides additional guidance for airplane-level failure classifications for part 23 airplanes. AC 25.1309 provides additional guidance for airplane-level failure classifications for part 25 airplanes.

(1) Hazardous Propeller Effect Failure Rates. The propeller safety analysis should show that hazardous propeller effects are not predicted to occur at a rate in excess of that defined as extremely remote (probability of 10^{-7} or less per propeller flight hour). AC 35.1, Certification of Propellers, provides additional guidance for individual failures and probabilities of this low order of magnitude. We note that a probability of 10^{-7} per propeller flight hour is not acceptable for some part 23 airplanes or for any part 25 airplanes. Those airplanes may require a rate of 10^{-9} or less per propeller flight hour. The applicant should establish the rate required per propeller flight hour based on the airplane installation early in the control development program. This will ensure that the airplane meets its certification requirements with the propeller installed.

(2) Major Propeller Effect Failure Rates. A summary should be made of all failures that could result in a major propeller effect along with the expected hourly failure rate of occurrence for those effects. AC 35.1, Certification of Propellers, provides further guidance on major propeller effects.

b. Supplemental Guidance for the Safety Analysis § 35.15.

(1) The safety analysis in § 35.15 should address all operating modes, and the data used in the safety analysis should be substantiated.

(2) The safety analysis should consider all faults, both detected and undetected, and their effects on the propeller control system and the propeller itself. The intent is primarily to address faults or malfunctions that affect only one propeller control system, and therefore only one propeller. However, the safety analysis should also include faults or malfunctions in airplane, engine, or propeller signals, including those in a multi-engine installation that could affect more than one propeller.

(3) The propeller control system safety analysis (SSA) should identify the applicable assumptions and installation requirements and establish any limitations relating to propeller control system operation. The propeller instructions for installation and operation should state these assumptions, requirements, and limitations.

(4) If the safety analysis assumes a particular crew action would reduce the impact of a fault condition, the instructions for propeller installation and operation should clearly state the assumed crew action, and the acceptability of those crew actions should be evaluated during airplane certification.

(5) The safety analysis should address all failures identified in § 35.15 that could result in major or hazardous propeller effects. The applicant should provide a summary that lists the malfunctions or failures, as well as their effects and the expected per hour rate of occurrence for the event, caused by the propeller control system.

(6) The safety analysis should also consider all signals used by the propeller control system, in particular any cross-propeller control signals. The airplane applicant needs to define the criticality of functions included in the propeller control system for airplane level functions.

(7) Where adequate validation data is not available, and extra conservatism is built into the analysis, then a normal post-certification in-service follow-up may be performed to obtain the data necessary to alleviate any consequence of the extra conservatism. This data may be used, for example, to extend system check intervals.

c. Criteria. The safety analysis should demonstrate or provide the following:

(1) Compliance with § 35.15.

(2) Failures leading to major propeller effects must show compliance with the agreed major propeller effects rates for the intended installation.

(3) Information on the consequence of the transmission of a faulty parameter by the propeller control system. Any information necessary to mitigate the consequence of a faulty parameter transmission should be contained in the propeller operating instructions.

d. Malfunctions or Faults Affecting Speed or Torque.

(1) When operating in the take-off envelope, uncovered faults in the propeller control system that result in a speed or torque change of less than +/- 3% are generally considered acceptable. However, this does not affect the applicant's obligation to ensure that the full-up system is capable of providing the declared minimum rated speed or torque. In this regard, faults that could result in small thrust changes should be random in nature and detectable and correctable during routine inspections, overhauls, or power-checks.

(2) In an airplane installation, the receiving propeller control system should provide authority limits on the signals sent from one propeller control system to another so that undetected faults do not result in an unacceptable change in speed or torque on the propeller using those signals. An example of this are the signals used for an automatic takeoff power control system (ATPCS), and auto feather control system, or synchrophasing.

(3) When operating in the take-off envelope, detected faults in the propellers control system that result in a speed or torque change of above +/- 3% may be acceptable if the total frequency of occurrence and magnitude for these types of failures is relatively low. The safety analysis should contain the predicted frequency of occurrence for this category of faults. The requirements for the allowable frequency of occurrence and magnitude for this category of faults and any need for a flight deck indication of these conditions should be reviewed during airplane certification.

(4) Detected faults in signals exchanged between propeller control systems should not result in greater than a +/- 3% speed or torque change on the propeller using the cross-propeller signals.

e. Commercial or Industrial Grade Electronic Parts.

(1) The grade and handling of electronic parts is an important contributor to the reliability of the EPCS. Two examples of industry documents that provide guidance on the application of commercial or industrial grade components are:

(a) IEC/TS 62239, Process Management for Avionics – Preparation of an Electronic Components Management Plan, and

(b) IEC/TR 62240, Process Management for Avionics - Use of Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges.

(2) When the propeller type design specifies commercial or industrial grade electronic components, and not manufactured to military standards, the applicant should have the following data available for review, as applicable:

(a) Reliability data for each commercial and industrial grade electrical component specified in the design.

(b) The applicant's procurement, quality assurance, and process control plans for the vendor-supplied commercial and industrial grade parts. These plans should ensure that the parts will be able to maintain the reliability level specified in the approved propeller type design.

(c) Unique databases for similar components obtained from different vendors because commercial and industrial grade parts may not all be manufactured to the same accepted industry standard.

(3) Commercial and industrial grade parts have typical operating ranges of 0^0 to $+70^0$ Celsius and -40^0 to $+85^0$ Celsius, respectively. Military grade parts are typically rated at -54^0 to 125^0 Celsius. Commercial and industrial grade parts are typically defined in these temperature ranges in vendor parts catalogues. If the declared temperature environment for the propeller control system results in commercial or industrial grade electronic components exceeding their stated capability, the applicant should:

(a) Determine the temperature range for the component;

(b) Substantiate that the component is suitable for operation; and

(c) Adjust the failure rates used for those components in the SSA.

(4) Additionally, if commercial or industrial parts are used in an environment beyond their specified rating and cooling provisions are required in the design of the EPCS, the applicant should specify these provisions in the propeller installation instructions to ensure that the provisions for cooling are not compromised. The cooling provisions included in the EPCS design may have failure modes. If failures could result in exceeding the temperature limits, the applicant should account for the probability of these failures in the SSA analysis.

(5) When any electrical or electronic components are changed, the applicant should review SSA analysis with regard to the impact of any changes in component reliability. Component, subassembly or assembly level testing may be needed to substantiate a change that introduces commercial or industrial part(s). However, such a change would not be classified as "significant" with respect to § 21.101(b)(1).

12. Section 35.23(b)(1) – Single Fault Accommodation. The applicant should substantiate single failure specifications by a combination of tests and analyses. It is intended that single failures or malfunctions in the propeller control system's components, in its fully operational condition and all declared dispatchable configurations, do not result in a hazardous propeller effect. In addition, for an EPCS in its full-up configuration, the control system should be "essentially single fault tolerant" of electrical/electronic component failures. We recognize, however, that to achieve true single fault tolerance would require either a triplicate design approach or a design approach with 100 % fault detection. Currently, systems are designed with dual, redundant channels or with back-up systems that provide what has been called an "essentially single fault tolerant" system.

13. Section 35.23(b)(2) – Local Events.

a. Examples of Local Events Include:

(1) Overheat conditions;

(2) Fires;

(3) Fluid leaks;

(4) Maintenance and foreseeable maintenance errors such as using a wire bundle as a hand hold; or

(5) Mechanical disruptions that could lead to damage of control system mechanical linkages, electrical harnesses, connectors, or the control itself.

b. Considerations for local events are:

(1) Local events normally affect only one propeller. Therefore, a local event is not usually considered a common mode event, which affects more than one propeller. Common mode threats, such as HIRF and rain, are not normally considered local events.

(2) Invalid assumptions of independence between failures as well as failure to recognize common cause failure modes are leading reasons invalid conclusions are reached within safety analyses. In the assessment of local events, emphasis should be placed on identifying and assuring critical functional or physical isolation is maintained. Then a zonal and/or other common cause/mode analyses can be conducted to assure that there is no common cause event that would violate any of those assumptions. For example:

(a) Control components required for feathering are not impacted by the same event(s) that could cause an engine failure (for example, fuel leak/fire) or the engine failure itself (for example, turbine engine uncontained failure); and

(b) Pitch control components whose failure could result in overspeed are not impacted by the same event(s) that could cause loss of overspeed protection.

(3) During a local event, the behavior of the propeller control system should not cause a hazardous propeller effect in any approved dispatchable mode.

(4) When demonstrating that no hazardous propeller effect exists based on the assumption that another function exists to provide the necessary protection, the applicant should show that this function is not rendered inoperative by the same local event on the propeller (including destruction of wires, power supplies, and linkages).

(5) An overheat condition exists when the temperature of the system components is greater than the maximum safe design operating temperature for the components, as declared by the applicant in the propeller instructions for installation. When the components of the propeller control system are exposed to an overheat condition, the system should not cause a hazardous propeller effect. This includes the recovery after the heat source is removed. The applicant may use specific design features or analysis methods to show compliance to the prevention of hazardous propeller effects. When this is not possible, due for example to the variability or complexity of the failure sequence, then we may require testing.

(6) We recognize that it is difficult to address all possible local events in the intended airplane installation at the time of propeller certification. Therefore, the applicant should apply sound engineering judgment to identify reasonably foreseeable local events. The applicant may show compliance with this specification by considering the end result of the local event on the propeller control system. The applicant should clearly document the analyzed local events to aid in certification of the propeller installation.

(7) The applicant should assess by analysis or test the effects of hydraulic or lubricating leaks impinging on components of the propeller control system. Such conditions should not result in a hazardous propeller effect, nor should the fluids be allowed to impinge on circuitry or printed circuit boards that could result in a potential latent failure condition.

c. The following guidance applies to propeller control system wiring:

(1) Each wire or combination of wires interfacing with the EPCS that could be affected by a local event should be tested or analyzed with respect to local events. The assessment should include open circuits, shorts to ground, and shorts to power (when appropriate). The results should show that faults result in specific responses and do not result in hazardous propeller effects. In addition, the applicant should show that any EPCS component connector that becomes disconnected while the propeller is operating does not cause a hazard to the continued safe flight and landing of the airplane.

(2) The applicant should test or analyze propeller control unit airplane interface wiring for shorts to airplane power; these "hot" shorts should result in a specific and non-hazardous propeller effect. Where airplane interface wiring is involved, the propeller installation instructions

should inform the installer of the potential effects of shorts in the interface wiring. The installer should ensure that no wiring faults exist that:

(a) Are not detectable and not accommodated; or

(b) Could result in a hazardous propeller effect.

(3) Where practical, wiring faults should not affect more than one channel. The propeller applicant should include any assumptions regarding channel separation in the SSA analysis.

(4) Where physical separation of conductors is not practical, the propeller applicant and the installer should coordinate to ensure that the potential for common mode faults between propeller control systems is eliminated and between channels on one propeller is minimized.

(5) The applicant should assess, by analysis or test, the effects of fluid leaks impinging on components of the EPCS. Such conditions should not result in a hazardous propeller effect, and the fluids may not be allowed to impinge on circuitry or printed circuit boards or result in a potential latent failure condition.

14. Section 35.23(b)(3) – Back-Up Systems. The propeller should have a protection system or back-up devices, such as an overspeed governor, counter weights, pitch lock, high pitch or low pitch stop. Two categories of malfunction should be considered. Those resulting from external causes such as engine failures and airplane flight conditions, and those caused by propeller control system failures. If a control system protection function is necessary, then the protection system should be evaluated with regard to its functionality and reliability as part of the propeller control system.

a. The combined normal or primary propeller control and protection system should be at least two faults or failures removed from a potential hazardous propeller effect. For example, a single failure mode should not result in unintended movement below the in-flight low pitch position. In this case, a potential overspeed or high drag condition will only be possible as a result of the initial fault causing a low pitch command and an independent fault preventing the protection system from operating.

b. The analysis should show that the hourly failure rate per occurrence of a control system failure condition from any cause in combination with failures of the appropriate protection system is less than 10^{-9} for part 25 applications. The failure rates for part 23 airplanes range from 10^{-7} to 10^{-9} or less. AC 23.1309-1C provides additional guidance for part 23 airplanes. The applicant should establish an overall hourly failure rate per occurrence for the intended installation to ensure that the propeller is installable. Some installations require that a probability of 10^{-9} per hour be shown for unintended movement below the in-flight low pitch position.

c. The probability of the protection system failing to operate when required should be on the order of 10^{-4} or less per flight hour.

d. The probability of an inadvertent operation of the protection system should be commensurate with the failure consequences.

e. Dedicated protection systems that are provided to prevent hazardous propeller effects are a necessary function for dispatch. Therefore, the applicant should test the protection system in a manner commensurate with the intended installation and the reliability of the protection system.

15. Section 35.23(b)(4) – Shared Data or Signals. In the exchange of data with the airplane, consideration should be given to eliminate unacceptable common mode faults affecting the operation of more than one engine or propeller. Common faults that affect propeller protection limit systems or could hazard the airplane are generally unacceptable. In particular, the applicant should consider the following:

a. Erroneous data received from the airplane or engine by the propeller control system if the data source is common to more than one propeller (for example, air data sources, synchronizing controls).

b. Control system operating faults propagating via data links between propellers (for example, maintenance recording, common bus, cross-talk, auto-feathering, and ATPCS implementation).

c. Loss or interruption of airplane data or electrical power used by the propeller control when that loss or interruption is caused by the failure of another propeller system.

d. Exchange of data between propellers to implement control functions (for example, synchrophasing) should be shown to incorporate authority limits to prevent unacceptable common mode loss of control.

e. Logic included in the control system to accommodate the faults considered in paragraphs 15.a. through d. above should be demonstrated. Any precautions needed to address common effects may be taken either through the airplane system architecture or by logic internal to the propeller control system. The instructions for propeller installation and operation should describe these precautions. The applicant may demonstrate this as part of the propeller control system validation test program.

16. Section 35.23(c) – Software Design and Implementation.

a. Objective.

(1) For propeller control systems that use embedded software the objective is to prevent as far as possible logic errors that would result in an unacceptable effect on pitch, speed and torque, or in other unsafe conditions. Because of the nature and complexity of systems containing digital logic, the software should be developed using a structured development approach, commensurate with the hazard associated with failure or malfunction of the system in which the digital logic is contained.

(2) Applicants may not be able to establish with certainty that the software has been designed without errors. However, if the applicant uses the software level or the hardware design assurance level appropriate for the criticality of the performed functions and uses an approved development method, the software satisfies the requirement to minimize errors. In multiple propeller installations, the possibility of digital logic errors common to more than one propeller control system may determine the criticality level of the software. However, the need for dissimilar designs has not been required when Level A is used.

b. Approved Methods. The primary FAA guidance on software methods is found in AC 20-115B and in FAA order 8110.49. For acceptable methods in developing software, comply with the guidelines of documents RTCA DO-178B/EUROCAE ED-12B, ,referred to as DO-178B. Alternative methods for developing software may be proposed by the applicant and are subject to approval by the Administrator.

c. Level of Software.

(1) Determination of the appropriate software level may depend on the failure modes and consequences of those failures. For example, it is possible that failures resulting in significant pitch change or speed oscillations may be more severe than a failure to a fixed pitch and should be considered when selecting a given software level.

(2) In multiple propeller installations to be type certificated under part 25 transport or part 23 commuter airplanes, the design, implementation and verification of software in accordance with Level A (DO-178B) is normally needed to achieve the certification objectives for the airplane.

(3) The criticality of functions on other airplanes may be different, and therefore, a different level of software design assurance may be acceptable.

(4) For propellers on reciprocating engines, the following guidelines have been set:

(a) Software level C has been determined to be the minimum requirement for a non-reversing and non-feathering propeller on a reciprocating engine EPCS.

(b) For reciprocating engine EPCS installed in airplanes approved under part 23 commuter or part 25 transport categories, the minimum software level for those EPCS should be determined by performing an airplane system-level safety analysis.

(c) For reciprocating engine EPCS installed in any other airplane, the applicant should evaluate the failure condition criticality of EPCS functions to determine if Level C software would be adequate. This would require coordination with the airplane designer and the cognizant FAA Aircraft Certification Office (ACO) during the EPCS development program.

(5) Applicants may protect or partition non-critical software from critical software and design and implement the non-critical software to a lower level. The applicant should

demonstrate the adequacy of the partitioning method as well as the protection and isolation features needed to prevent corruption between the two levels of software. This demonstration should consider whether the protected/partitioned lower software levels are appropriate for any anticipated installations. Should the criticality level be higher in subsequent installations, the applicant would need to meet all requirements for the higher software level.

d. Onboard or Field Loadable Software and Part Number Marking. Use the following guidelines and refer to FAA order 8110.49 when onboard or field loading of electronic propeller control software and associated EPM is implemented:

(1) For software changes, document the software to be loaded by an approved design change and released with a service bulletin or other appropriate documentation.

(2) For an EPCS unit with separate part numbers for hardware and software, the software part number(s) need not be displayed on the unit as long as they are embedded in the loaded software and can be verified by electronic means. When new software is loaded into the unit, the same verification requirement applies and the proper software part number should be verified before the unit is returned to service.

(3) For an EPCS unit with only one part number, the single part number represents a combination of a software and hardware build. Applicants should change or update the unit part number on the nameplate when the new software is loaded. The software build or version number should be verified before the unit is returned to service.

(4) For an EPCS that will be onboard or field loaded, the configuration control system and the use of EPM should be approved. The drawing system should provide a compatibility table that tabulates the combinations of hardware part numbers and software versions that have been approved by the Administrator. The top-level compatibility table should be under configuration control, and it should be updated for each change that affects hardware/software combinations. The applicable service bulletin should define the hardware configurations with which the new software version is compatible.

(5) The loading system should be in compliance with the guidelines of DO-178B, Section 2.5. If the applicant proposes more than one source for loading, (for example, diskette or mass storage), all sources should comply with these guidelines.

(6) The service bulletin should require verification that the correct software version has been loaded after installation on the airplane.

e. Software Change Category. The processes and methods used to change software should not affect the design assurance level of that software.

(1) The determination of major change versus minor change is established in § 21.93. A change to the software in a propeller control system may affect the reliability, operational characteristics, or other characteristics affecting the airworthiness of the product and is, therefore,

normally classified as a major change. Paragraphs (2) and (3) below provide additional guidance regarding classification of software changes.

(2) The failure effect of EPCS software is always assumed to have a major effect because an error could result in a hazardous or major propeller effect. Therefore, software changes are almost always classified as a major change. Exceptions are decided on a case-by-case basis. Therefore, a change to software produced in accordance with DO-178B should be classified as a major change if any of the following applies and the failure effect is categorized as catastrophic, hazardous or major:

(a) The executable code for software, determined to be Level A or B in accordance with DO-178B, is changed, unless that change involves only a variation of a parameter value within a range already verified for the previous certification standard;

(b) The software is upgraded to, or downgraded from, Level A, B or C; or

(c) The executable code, determined to be Level C, is substantially changed. For example, after adding a function or after a software reengineering process accompanying a change of processor.

(3) For software developed to processes other than DO-178B, the applicant should assess changes in accordance with the system principles established in §§ 23.1309 or 25.1309 and coordinated with the cognizant ACO. For systems assessed under §§ 23.1309 or 25.1309, the classification process is based on the functional aspects of the change and its potential effects on safety. The following guidance applies:

(a) When the failure effect at the airplane level is "catastrophic" or "hazardous," the change should be classified as a major change.

(b) When the failure effect at the airplane level is "major", the change should be classified as a major change if:

1. Aspects of the compliance demonstration uses means not previously accepted for the nature of the change to the system;

2. The change affects the pilot/system interface (displays, controls, approved procedures); or

3. The change introduces new types of functions/systems.

f. Software Changes by Others than the TC Holder.

(1) Software changes by someone other than the original TC holder are generally not feasible. The applicant should address the approval process with the certification authority to determine feasibility.

(2) Two types of software changes exist that could be implemented by someone other than the original TC holder. The two types are option-selectable software, or user-modifiable software (UMS).

(a) Option-selectable changes are pre-certified logic that uses a method of selection shown not to be capable of causing a control malfunction.

(b) UMS is software intended for modification by the airplane operator without review by the certification authority, the airplane applicant, the propeller manufacturer, or the equipment vendor. For propeller control systems, UMS has generally not been applicable. However, approval of UMS, if required, would be addressed on a case-by-case basis.

(3) The necessary guidance for UMS is contained in DO-178B, paragraph 2.4. The guidance allows non-TC holders to modify the software within the modification constraints defined by the TC holder if the system has been certified with the provision for software user modifications. To certify an EPCS with the provision for software modification by a non-TC holder, the TC holder should (1) provide the necessary information for approval of the design and implementation of a software change; and (2) demonstrate that the necessary precautions have been taken to prevent the user modification, regardless of whether it is implemented correctly, from affecting propeller airworthiness.

(4) When the software is changed in a manner not allowed by the TC holder as "user modifiable," the non-TC holder applicant should comply with all the specific applicable requirements of 14 CFR 35; and in particular all the provisions of § 35.23 as well as the requirements in part 21, subpart E. Refer to FAA order 8110.49, particularly Chapter 7, "Approval of Airborne Systems and Equipment Containing User-Modifiable Software (UMS)" for additional information.

17. Section 35.23(d) – Airplane-Supplied Data.

a. Context. Airplane-supplied data, in this context, includes all analog, discrete, and digital data provided by airplane systems to the EPCS. Engine-supplied data is a subset of airplane-supplied data.

b. Items to Address. When airplane-supplied data can affect propeller control system operation, the applicant should address the following items, as applicable, in the safety analysis or other appropriate documents:

(1) Software and complex electronic hardware in the data path to the EPCS should be at a level consistent with the criticality of the EPCS function that uses that data. The data path may include other airplane avionics.

(2) The applicant should state in the instructions for installation that the airplane applicant is responsible for ensuring that changes to airplane avionics units, including software, in the data

path to the EPCS do not affect the integrity of the data provided to the propeller as defined by the EPCS instructions for installation.

(3) The applicant should provide the effects of faulty and corrupted airplane-supplied data on the EPCS in the propeller instructions for installation.

(4) The instructions for installation should state the installer should ensure those sensors that deliver information to the EPCS are capable of operating in "severe" HIRF and lightning environments, as defined in the certification basis for the airplane, without affecting their proper and continued operation.

(5) The applicant should state the reliability level for airplane-supplied data used as part of the safety analysis as an "assumed value" in the instructions for installation.

c. Additional Considerations.

(1) If the airplane command system is configured to move the propeller speed and torque levers or to transmit an electronic signal to command a speed or torque change, then the propeller control system merely responds to the command and changes to propeller speed and torque as appropriate. The propeller control system may have no way of detecting the sensed speed or torque lever movement was correct or erroneous. Faulty or erroneous airplane data should not have an adverse effect on propeller protection systems.

(2) In both the moving speed (or condition) lever and torque (or power) lever configurations, it is the installer's responsibility to show that a proper functional hazard analysis has been performed on the airplane system involved in generating propeller speed and torque commands. The installer should also show that the system meets the appropriate airplane's functional hazard assessment safety related specifications. This task is an airplane certification issue.

d. Design Assessment.

(1) The applicant should prepare a fault accommodation chart that defines the fault accommodation architecture for the airplane-supplied data.

(2) There may be elements of the propeller control system, such as a blade angle position resolver, that are mounted in the airplane and are not part of the propeller type design, but which are dedicated to the propeller control system and powered by it. In these instances, such elements are considered an integral component of the EPCS and are not considered airplane data.

(3) When particular failure modes of the airplane air data are unknown, the applicant should assume typical failure modes of loss of data and erroneous data. We are using the term "erroneous data" in this AC to describe a condition where the data appears to be valid, but is incorrect.

(4) The applicant should provide such assumptions and the results of the evaluation of erroneous airplane data to the installer.

(5) The following are examples of possible means of accommodation:

(a) Provision of an alternate mode that is independent of airplane-supplied data.

(b) Dual sources of airplane-supplied sensor data with local propeller sensors provided as voters and alternate data sources.

(c) Use of synthesized propeller parameters as voters. When synthesized parameters are used for control or voting purposes, the analysis should consider the impact of temperature and other environmental effects on those sensors whose data are used in the synthesis. The applicant should also assess the variability of any data or information necessary to relate the data from the sensors used in the synthesis to the parameters being synthesized.

(d) Triple redundant air data computer systems that provide the required data.

(6) If, for airplane certification, the applicant intends to show that the complete loss of the airplane air data system is extremely improbable, then the applicant should show the airplane air data system is unaffected by a complete loss of airplane generated power. An example would be an airplane power system that is backed up by battery power.

e. Validation.

(1) The applicant should demonstrate functionality of the fault accommodation logic by test, analysis, or a combination of both. When the airplane air data system is not functional because of the loss of all airplane generated power, the propeller control system should include validated fault accommodation logic that prevents the propeller from producing a hazardous propeller effect. Propeller operation in this system configuration should be demonstrated by test.

(2) For all dispatchable control modes, the next single fault should be shown not to lead to a hazardous propeller effect.

(3) If an alternate mode, independent of airplane-supplied data, has been provided to accommodate the loss of all data, the applicant should conduct sufficient testing to demonstrate that the operability specifications have been met when operating in this mode. The instructions for installation should include characteristics of operation in this mode, even if this is a non-dispatchable mode.

18. Section 35.23(e) – Airplane-Supplied Electrical Power.

a. Airplane-Supplied Electrical Power. Airplane-supplied electrical power should provide an electrical power source to the EPCS that is at a minimum single fault tolerant. The most common method of achieving this objective has been to provide an independent alternator as the electrical

power source for the EPCS. However, with the increased integration of propeller-airplane systems and with the application of EPCS to small propellers, both on reciprocating and turbine engines, use of an independent alternator may not necessarily be the only design approach to meet this objective. If airplane power faults or failures can contribute to major or hazardous propeller effects, these events should be included in the SSA. The instructions for installation should contain the assumed quality and reliability levels of airplane power. Engine-supplied power is a subset of airplane-supplied power.

b. Analysis of the Design Architecture.

(1) An analysis and review of the design architecture should identify the requirements for dedicated electrical power sources and airplane-supplied power sources. The analysis should include the sources of power and the effects of losing these sources. If the propeller depends on airplane-supplied power for any operational functions, the analysis should result in a definition of the requirements for airplane-supplied power.

(2) The capacity of any EPCS dedicated power source should provide sufficient margin to maintain confidence that the propeller control system will continue to function in all anticipated operating conditions where the control system is designed and expected to recover propeller operation in-flight. This margin should account for any other anticipated variations in the output of the dedicated power source, such as those due to temperature variations, manufacturing tolerances, and idle speed variations. The design margin should be substantiated by test, analysis, or both, and should take into account any deterioration over the life of the propeller.

(3) When compliance imposes a dedicated electrical power source, the SSA should address the failure of this source. While no credit is normally given in the SSA for the use of airplane-supplied electrical power as a back-up power source, airplane power has typically been used to accommodate the loss of the propeller's dedicated power supply. However, the FAA will review, on a case-by-case basis, any impact on the SSA for the use of airplane power as the power source for a propeller control back-up system.

(4) When airplane electrical power is necessary for operation of the propeller control system, the propeller instructions for installation should contain the propeller control system's electrical power supply quality and reliability requirements. This should include steady state and transient under-voltage and over-voltage limits for the equipment. The power input standards of DO-160F provide an acceptable definition of such requirements. If DO-160F is used, the applicant should state any exceptions to the power quality standards cited for the particular category of equipment specified.

(5) When airplane power is the primary source for the EPCS, we recognize that the electronic components of the propeller control system may cease to operate during some low voltage airplane power supply conditions beyond those required to sustain normal operation. However, the operation of the propeller control should never result in a hazardous propeller effect. In addition, low voltage transients outside the control system's declared capability should not:

(a) Cause permanent loss of function of the control system;

(b) Result in inappropriate control system operation that could cause the propeller to exceed any operational limits; or

(c) Cause the transmission of unacceptable erroneous data.

(6) When airplane power recovers from a low-voltage condition to a condition the control is expected to operate normally, the propeller control system should resume normal operation. The time interval associated with this recovery should be contained in the propeller instructions for installation. We recognize that airplane power supply conditions may lead to a propeller feather or condition that is not recoverable automatically. We will determine the acceptability of any non-recoverable propeller operating conditions that are the result of airplane power supply conditions at airplane certification.

(7) In some system architectures, a dedicated power source may not be required and an airplane-supplied electrical power supply may be acceptable as the sole source of power.

(a) One example is a system that consists of a primary electronic single channel and a full capability hydro-mechanical back-up system that meets all specifications and does not depend on airplane power that is independent of electrical power. In this architecture, loss or interruption of airplane-supplied power is accommodated by transferring control to the hydro-mechanical system. If fault accommodation credit is established to transfer the control to the hydro-mechanical back-up, assure the fault accommodation cannot prevent such a transfer.

(b) Another example is an airplane power system that could support a fly-by-wire flight control system. This power system may be acceptable as the sole source of power for an EPCS.

c. Electrical Power Sources.

(1) Use of two isolated/independent airplane buses as the means of compliance with this specification is acceptable.

d. Effects on the Propeller.

(1) When loss of airplane power results in a change in propeller control mode, the control mode transition should meet specifications of paragraph 18.d.(2) of this AC.

(2) When a dedicated power source is part of the system configuration, the loss of some propeller control functions that rely on airplane-supplied electrical power may still be acceptable. Acceptability is based on an evaluation of the change in propeller operating characteristics, current experience with similar designs, and/or the accommodation designed into the control system.

e. Validation. The applicant should demonstrate the effects of loss of airplane-supplied electrical power by propeller test, system validation test, bench test, or any combination.

19. Section 35.3(a)(1) – Instructions for Propeller Installation and Operation.

a. Control System Description. The applicant should include a brief control system description and may reference a more detailed system description document.

b. Interface Description. The description should specify all of the physical, electrical, and functional interface requirements of the control system. The following types of information should be included for an EPCS:

(1) EPCS power requirements and quality, including interrupt limitations.

(2) Impedance and buffering limitations for the signals provided by the EPCS for display and instrumentation.

(3) Signals used by the EPCS, such as air data information. This is to ensure that the EPCS is adequately isolated and unaffected by other systems using these signals.

(4) Subtle interface requirements, such as power interrupt tolerance of the EPCS.

(5) Control system output information for maintenance to the cockpit, and fault information.

c. Operational Description. The instructions for installing and operating the propeller should contain a description of the control system operating characteristics in both the normal and alternate control and operating modes.

(1) Restrictions in the flight envelope or unusual operating characteristics in these alternate modes should be clearly defined and included in the operational description.

(2) Abnormal control characteristics that could affect crew procedures, training, workload, or any other aspects of airplane performance or operating characteristics should be identified and included for evaluation during airplane certification.

d. Substantiation Data. The applicant should, in the instructions for installing and operating the propeller, include or reference data from safety analyses, environmental testing, and software level determinations that will assist the installer to safely install the propeller.

e. Safety Analysis. The safety analysis should include the estimated reliability of, or the failure rates for, significant failure conditions and the other control system associated events, as determined in the SSA.

f. Environmental Testing. The types and levels of environmental exposure for which the control system has been successfully qualified (for example, vibration, temperature, HIRF, or lightning) should be stated. For the HIRF, lightning and EMI qualification tests, the interfacing airplane cables used for the tests should be stated.

g. Software and Airborne Electronic Hardware Validation and Verification. The documentation submitted in support of the software and airborne electronic hardware aspects of certification should be stated.

20. Airborne Electronic Hardware.

a. For propeller control systems that use airborne electronic hardware in the form of PLD or similar devices, the objective is to prevent errors that would result in an unacceptable effect on pitch, speed and torque, or in other unsafe conditions. Because of the nature and complexity of systems containing digital logic, the PLDs should be developed using a structured development approach that is equivalent to the hazard associated with the failure or malfunction of the system in which the digital logic is contained.

b. Applicants may not be able to establish with certainty that the PLD has been designed without errors. However, if the applicant uses the hardware design assurance level appropriate for the criticality of the performed functions and uses an approved development method, the PLD satisfies the requirement to minimize errors. In multiple propeller installations, the possibility of digital logic errors common to more than one propeller control system may determine the criticality level of the hardware design assurance level. However, the need for dissimilar designs has not been required when Level A is used.

c. Design Practices.

(1) Because of the nature and complexity of systems containing digital logic, PLDs should be developed using a structured development approach, corresponding with the hazard associated with failure or malfunction of the system in which the device is contained.

(2) RTCA DO-254/EUROCAE ED-80, describes standards for the criticality and design assurance levels associated with PLD development. This document describes an acceptable means, but not the only means, to show compliance. For systems requiring certification to levels higher than RTCA DO-254/EUROCAE ED-80 Level D, we may require additional validation and verification. AC 20-152, provides guidance when using RTCA DO-254.

(a) The primary FAA guidance on PLD methods is found in AC 20-152 and additional information is found in Order 8110.105 CHG 1. Methods for developing PLDs, compliant with the guidelines of document RTCA DO-254/EUROCAE ED-80 are acceptable. Alternative methods for developing PLDs may be proposed by the applicant and are subject to approval by the Administrator.

END